Failure Modes, Effects and Diagnostic Analysis

Project:
Ball Valve

Company:
Emerson Process Management Virgo Valves SRL
Milan
Italy

Contract Number: Q15/08-044
Report No.: VIR 08/01-53 R001
Version V2, Revision R2, December 8, 2015
Chris O'Brien - Steven Close

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Ball Valve. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the Ball Valve. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Ball Valve is a ¼ turn ball valve used to control process fluids. Emerson Process Management Virgo Valves SRL manufactures ball valves from 2" to 72" in size with pressure ratings up to ANSI 2500 or API 15000. Product variations include; Soft Seated, Metal Seated - bolted side entry, welded side entry, bolted top entry, underground, and subsea. The Ball Valve is designed to meet international standards including API 6D, API 6A and API 608 for design/construction including pressure and temperature ratings, shell thickness, and bore diameters. The Ball Valve provides ISO 5211 mounting for simple actuator mounting. The Ball Valve includes double body-gasket sealing and multiple stem seals. Table 1 gives an overview of the different versions that were considered in the FMEDA of the Ball Valve.

Table 1 Version Overview

Option 1	Ball Valve
Option 2	Underground Ball Valve
Option 3	Cryogenic Ball Valve

Failure rates for options 2 and 3 are listed in Appendix A. The Ball Valve is classified as a Type A[1] device according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H (see Section 5.2). Therefore the Ball Valve can be classified as a 2_H device when the listed failure rates are used. When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H. If Route 2_H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1_H.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

A user of the Ball Valve can utilize these failure rates in a probabilistic model of a Safety Instrumented Function (SIF) to determine suitability in part for Safety Instrumented System (SIS) usage in a particular Safety Integrity Level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

[1] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Ball Valve. From this, failure rates and example PFD_{avg} values may be calculated.

The information in this report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PFD_{avg}) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

A FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 400 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

2.2 Roles of the parties involved

Emerson Process Management Virgo Valves SRL	Manufacturer of the Ball Valves
exida	Performed the hardware assessment.

Emerson Process Management Virgo Valves SRL contracted *exida* in February 2008 with the hardware assessment of the above-mentioned device and again in August 2015 with the re-assessment of the above mentioned device.

2.3 Standards and Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 Reference documents

2.4.1 Documentation provided by Emerson Process Management Virgo Valves SRL

[D1]	Assembly 48” – 600#, July 2007	Assembly Drawing
[D2]	Assembly 24” – 900#, May 2007	Assembly Drawing
[D3]	Assembly 24” – 600# - BW ext., April, 2008	Assembly Drawing
[D4]	Assembly 56” – 600# - Welded Body, February 2008	Assembly Drawing
[D5]	Top Entry 20” – 900#, October 2007	Assembly Drawing
[D6]	Top Entry 8” – 900#, Full Cryo, December 2007	Assembly Drawing
[D7]	Valvola A SFERA 18” – 300#, October 2007	Assembly Drawing

2.4.2 Documentation generated by *exida*

[R1]	VIR 15-08-044 FMEDA Virgo Europe Ball Valves.xls, 8/24/2015	Failure Modes, Effects, and Diagnostic Analysis – Ball Valve
[R2]	VIR 08-01-53 R001 V2 R2 FMEDA Virgo Europe Ball Valves, 12/08/2015	FMEDA report, Ball Valve (this report)

3 Product Description

The Ball Valve is a ¼ turn ball valve used to control process fluids. Emerson Process Management Virgo Valves SRL manufactures ball valves from 2" to 72" in size with pressure ratings up to ANSI 2500 or API 15000. Product variations include; Soft Seated, Metal Seated - bolted side entry, welded side entry, bolted top entry, underground, and subsea. The Ball Valve is designed to meet international standards including API 6D, API 6A and API 608 for design/construction including pressure and temperature ratings, shell thickness, and bore diameters. The Ball Valve provides ISO 5211 mounting for simple actuator mounting. The Ball Valve includes double body-gasket sealing and multiple stem seals. Table 2 gives an overview of the different versions that were considered in the FMEDA of the Ball Valve.

Figure 1 defines the boundaries for FMEDA.

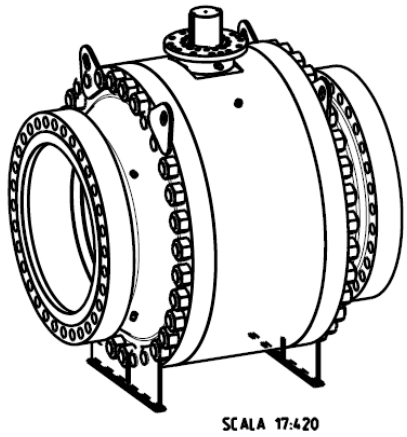


Figure 1 Ball Valve, Parts included in the FMEDA

Table 5 gives an overview of the different versions that were considered in the FMEDA of the Ball Valve.

Table 2 Version Overview

Option 1	Ball Valve
Option 2	Underground Ball Valve
Option 3	Cryogenic Ball Valve

The Ball Valve is classified as a Type A[2] device according to IEC 61508, having a hardware fault tolerance of 0. The complete final element subsystem, including the Ball Valve will need to be evaluated to determine the Safe Failure Fraction.

[2] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Emerson Process Management Virgo Valves SRL.

4.1 Failure Categories description

In order to judge the failure behavior of the Ball Valve, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the valve performs the safety function to open or close (depending on the application).
Full Stroke	State where the valve is closed.
Tight-Shutoff	State where the valve is closed and sealed with leakage no greater than the defined leak rate. Tight shut-off requirements shall be specified according to the application. If shut-off requirements allow flow greater than ANSI class V, respectively ANSI class VI, then Full Stroke numbers may be used.
Open on Trip	State where the valve is open.
Fail Safe	Failure that causes the (sub)system to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that is detected by an automatic diagnostic (such as Partial Valve Stroke Testing).
Fail Dangerous	A Failure that prevents the valve from moving to the defined fail-safe state within the normal time span.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics (such as Partial Valve Stroke Testing).
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.
External Leakage	Failure that causes process fluids to leak outside of the valve. External leakage is not considered part of the safety function and therefore this failure rate is not included in the Safe Failure Fraction calculation.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2000, the Residual failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

External leakage failure rates do not directly contribute the reliability of a valve but should be reviewed for secondary safety and environmental issues.

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] which was derived using over 100 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 3 (General Field Equipment) and Profile 6 (Process Wetted Parts) for the Valves process wetted parts, see Appendix D. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Emerson Process Management Virgo Valves SRL. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air hydraulic fluid quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related wearout failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix D. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Ball Valve.

- Only a single component failure will fail the entire Ball Valve
- Failure rates are constant, wear-out mechanisms are not included
- Propagation of failures is not relevant
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded
- The stress levels are average for an industrial environment and can be compared to the IEC 60654-1, Class Dx (outdoor location) with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Materials are compatible with process conditions
- The device is installed per manufacturer's instructions
- Valves are installed such that the controlled substance will flow through the valve in the direction indicated by the flow arrow, located on the valve body.
- The valves are generally applied in relatively clean gas or liquid, therefore no severe service has been considered in the analysis.
- Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test.
- Partial Valve Stroke Testing of the SIF includes position detection from actuator top mounted position sensors.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- Worst-case internal fault detection time is the PVST test interval time

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Ball Valve FMEDA.

The failure rates for the Ball Valve with are listed in Table 3.

Table 3 Failure rates Ball Valve

Failure Category	Failure Rate (FIT)		
	Full Stroke	Tight-Shutoff	Open to Trip
Fail Safe Detected	0	0	0
Fail Safe Undetected	0	0	189
Fail Dangerous Detected	0	0	0
Fail Dangerous Undetected	691	1272	502
Residual	680	99	680

The failure rates for the Ball Valve with PVST are listed in Table 4.

Table 4 Failure Rates Ball Valve with PVST

Failure Category	Failure Rate (FIT)		
	Full Stroke	Tight-Shutoff	Open to Trip
Fail Safe Detected	0	0	0
Fail Safe Undetected	0	0	189
Fail Dangerous Detected	283	283	283
Fail Dangerous Undetected	408	989	219
Residual	680	99	680

In addition to the failure rates listed above, the external leakage (Valve process media) failure rate of the Ball Valve is 438 FIT. As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure rates do not directly contribute to the reliability of the valve but should be reviewed for secondary safety and environmental issues.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508 (see Section 5.2).

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore the Ball Valve meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

Table 5 lists the failure rates for the Ball Valve according to IEC 61508.

Table 5 Failure rates according to IEC 61508, FIT

Device	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}
Full Stroke	0	0	0	691
Tight-Shutoff	0	0	0	1272
Open to Trip	0	189	0	502
Full Stroke with PVST	0	0	283	408
Tight-Shutoff with PVST	0	0	283	989
Open to Trip with PVST	187	2	283	219

The architectural constraint type for the Ball Valve is A. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

[3] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 PFD_{avg} calculation Ball Valve

Using the failure rate data displayed in section 4.4, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the entire final element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix E for a complete description of how to determine the Safety Integrity Level for the final element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates for all the devices in the final element and the proof test coverage for the final element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test and the dangerous failure rate after proof test for the Ball Valve are listed in Table 13. This is combined with the dangerous failure rates after proof test for other devices in the final element to establish the proof test coverage for the final element.

When performing Partial Valve Stroke Testing at regular intervals, the Ball Valve contributes less to the overall PFD_{avg} of the Safety Instrumented Function.

5.2 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:

> "based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to
>
> - the amount of field feedback; and
> - the exercise of **expert judgment**; and when needed
> - the undertake of specific tests,
>
> in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508, ed2, 2010 does not give detailed criteria for Route 2_H, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and

2. a device and all of its components have been installed in the field for one year or more; and

3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and

4. failure definitions, especially "random" vs. "systematic" are checked by *exida*; and

5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.

6 Terms and Definitions

FIT	Failure In Time (1x10-9 failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PVST	Partial Valve Stroke Test
	It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Stroke Testing also has an impact on the Safe Failure Fraction.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	"Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version History:	V2, R2:	Revised company name and product description, Dec 8, 2015
	V2, R1:	Updated during surveillance audit per Q15/08-044, Aug 26, 2015
	V1, R2:	Updated product description, August 25, 2008
	V1, R1:	Released to Emerson Process Management Virgo Valves SRL; July 11, 2008
	V0, R1:	Draft; July 11, 2008
Author(s):	Chris O'Brien - Steven Close	
Review:	V2, R1:	Ted Stewart (exida), August 25, 2015
Release Status:	Released	

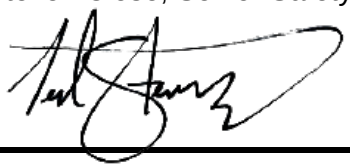
7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Chris O'Brien, Director of Business Development

Steven Close, Senior Safety Engineer



Ted E. Stewart, CFSP, Program Development & Compliance Manager

Appendix A Additional Failure Rates

Failure Rates for Underground Large Diameter Trunnion Ball Valves

Table 6 Failure Rates Underground Ball Valve

Failure Category	Failure Rate (FIT)		
	Full Stroke	Tight-Shutoff	Open to Trip
Fail Safe Detected	0	0	0
Fail Safe Undetected	0	0	189
Fail Dangerous Detected	0	0	0
Fail Dangerous Undetected	763	1344	574
Residual	710	129	710

Table 7 Failure Rates Underground Ball Valve with PVST

Failure Category	Failure Rate (FIT)		
	Full Stroke	Tight-Shutoff	Open to Trip
Fail Safe Detected	0	0	0
Fail Safe Undetected	0	0	189
Fail Dangerous Detected	304	304	304
Fail Dangerous Undetected	459	1039	270
Residual	710	129	710

Table 8 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}
Underground, Full Stroke	0	0	0	763
Underground, Tight-Shutoff	0	0	0	1344
Underground, Open to Trip	0	189	0	574
Underground, Full Stroke with PVST	0	0	304	459
Underground, Tight-Shutoff with PVST	0	0	305	1039
Underground, Open to Trip with PVST	0	189	304	270

[4] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

Table 9 Failure rates Ball Valve

Failure Category	Failure Rate (FIT)		
	Full Stroke	Tight-Shutoff	Open to Trip
Fail Safe Detected	0	0	0
Fail Safe Undetected	0	0	171
Fail Dangerous Detected	0	0	0
Fail Dangerous Undetected	707	1288	536
Residual	705	124	705

Table 10 Failure Rates Ball Valve with PVST

Failure Category	Failure Rate (FIT)		
	Full Stroke	Tight-Shutoff	Open to Trip
Fail Safe Detected	0	0	0
Fail Safe Undetected	0	0	171
Fail Dangerous Detected	265	267	265
Fail Dangerous Undetected	442	1021	271
Residual	705	124	705

Table 11 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU} [5]	λ_{DD}	λ_{DU}
Cryogenic, Full Stroke	0	0	0	707
Cryogenic , Tight-Shutoff	0	0	0	1288
Cryogenic , Open to Trip	0	171	0	536
Cryogenic , Full Stroke with PVST	0	0	265	442
Cryogenic , Tight-Shutoff with PVST	0	0	267	1021
Cryogenic , Open to Trip with PVST	0	171	265	271

[5] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

Appendix B Lifetime of Critical Components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[6] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is the responsibility of the end user to maintain and operate the Ball Valve per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 10 to 15 years is expected for the Ball Valve.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[6] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix C Proof tests to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

C.1 Suggested Proof Test

The suggested proof test consists of a full stroke of the Large Diameter Trunnion Ball Valve, as described in Table 15. The remaining dangerous failures after performing the suggested proof test are listed in Table 13 along with the proof test coverage both with and without PVST.

Table 12 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Send a signal to the final element configuration to perform a full stroke and verify that this is achieved.
3.	Inspect the Ball Valve for any visible damage or contamination.
4.	Remove the bypass and otherwise restore normal operation.

C.2 Proof Test Coverage

The Proof Test Coverage for the various device configurations is given in Table 13.

Table 13 Proof Test Results – Ball Valve

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
		No PVST	with PVST
Full Stroke	224	68%	45%
Tight-Shutoff	802	37%	19%
Open to Trip	35	93%	84%
Underground, Full Stroke	295	61%	36%
Underground, Tight-Shutoff	874	35%	16%
Underground, Open to Trip	106	81%	61%
Cryogenic, Full Stroke	315	55%	29%
Cryogenic , Tight-Shutoff	893	31%	13%
Cryogenic , Open to Trip	144	73%	47%

Appendix D *exida* Environmental Profiles

Table 14 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[7]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[8]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[9]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[10]	G2	G3	G3	G3	G3	Compatible Material
Surge[11]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[12]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[13]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[7] Humidity rating per IEC 60068-2-3
[8] Shock rating per IEC 60068-2-27
[9] Vibration rating per IEC 60068-2-6
[10] Chemical Corrosion rating per ISA 71.04
[11] Surge rating per IEC 61000-4-5
[12] EMI Susceptibility rating per IEC 61000-4-3
[13] ESD (Air) rating per IEC 61000-4-2

Appendix E Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). **The numbers used in the examples are not for the product described in this report.**

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N5] and [N8].

These are:
A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;
B. Architecture Constraints (minimum redundancy requirements) are met; and
C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N9].

C. Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD_{avg}) must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restore (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03 (Figure 2).

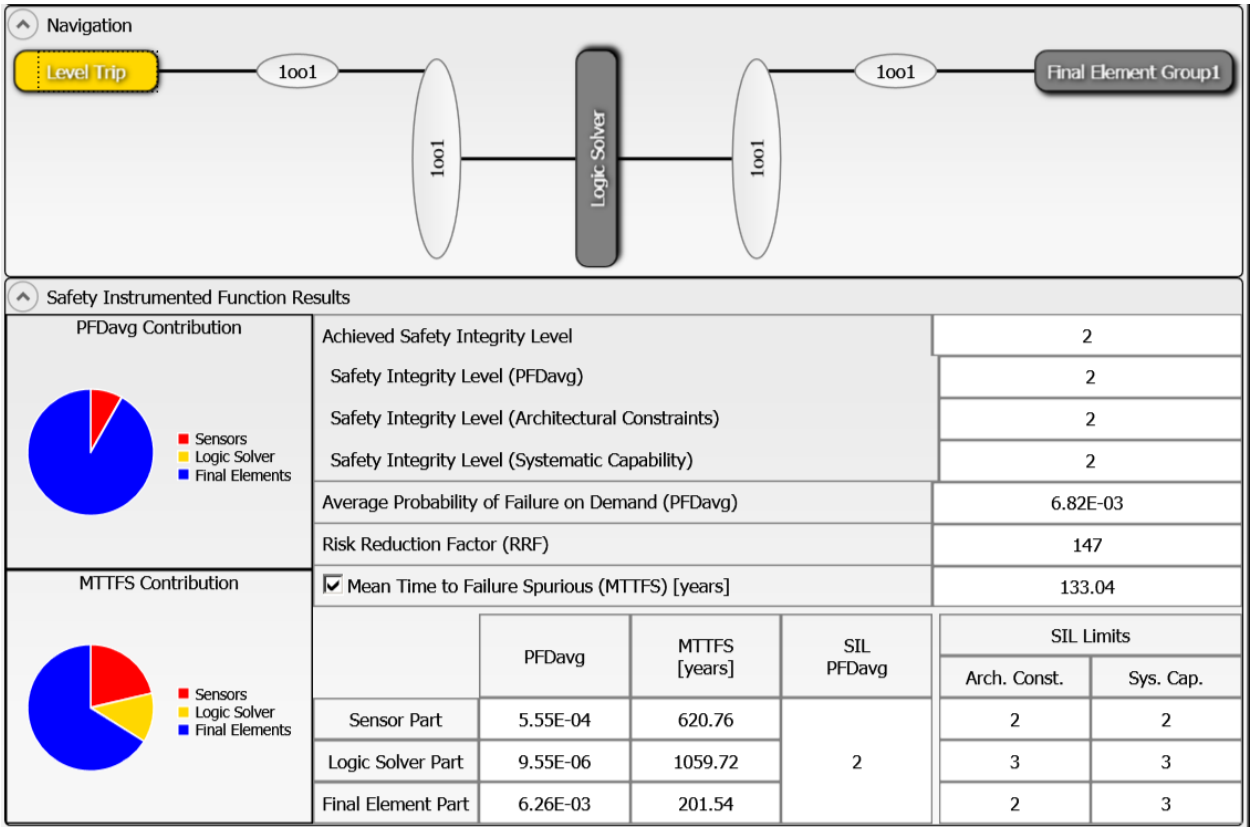


Figure 2: exSILentia results for idealistic variables.

If the Proof Test Internal for the sensor and final element is increased in one year increments, the results are shown in Figure 3.

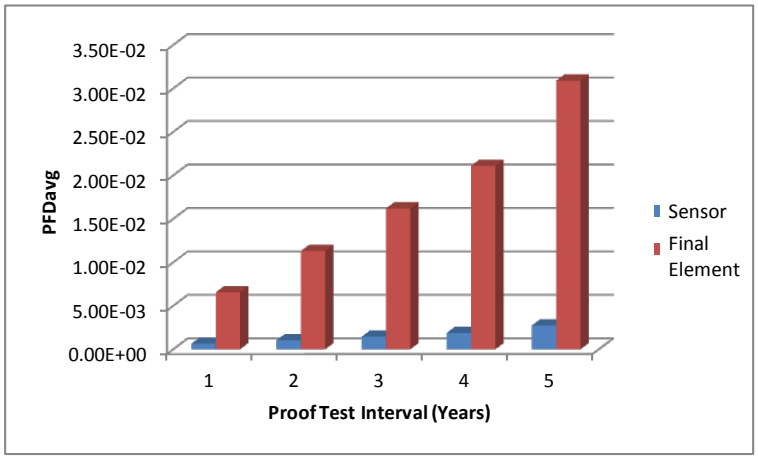


Figure 3: PFD_{avg} versus Proof Test Interval

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 4).

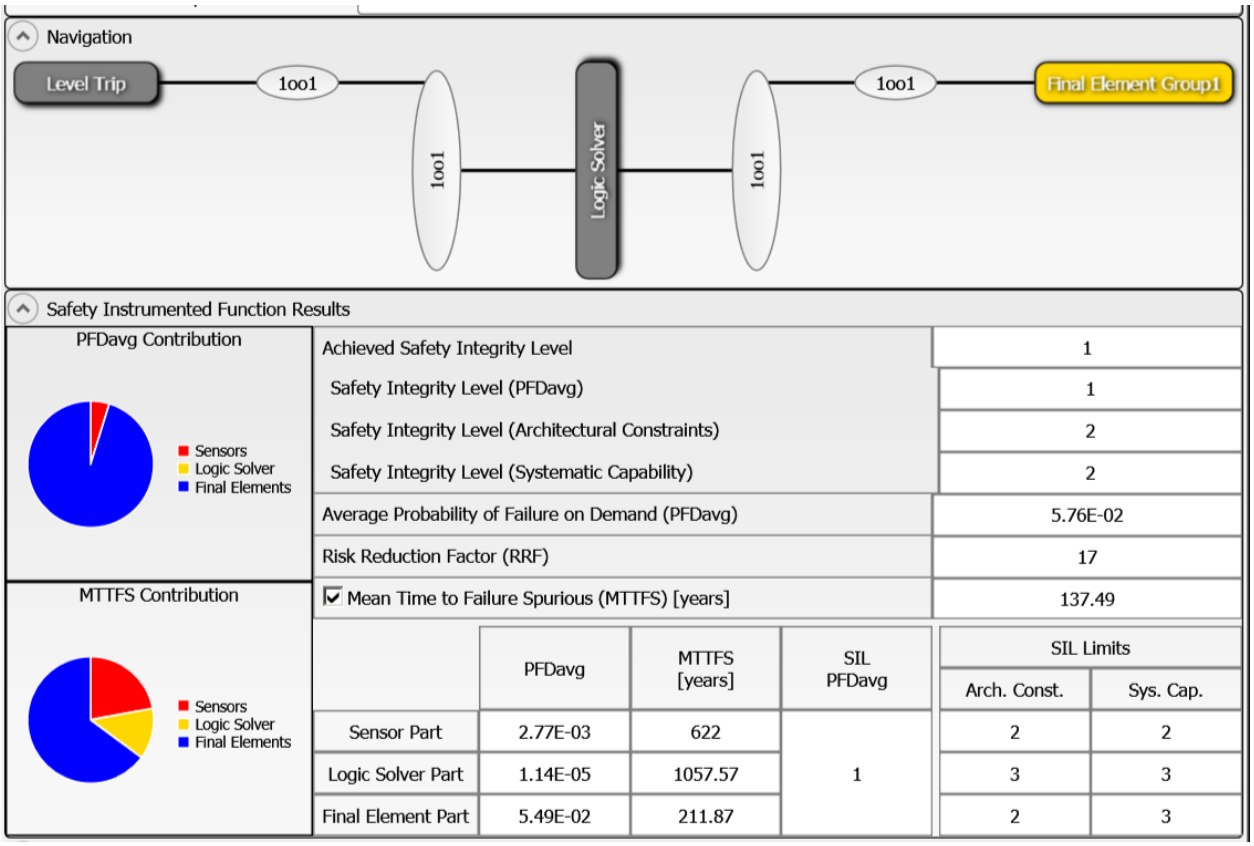


Figure 4: exSILentia results with realistic variables

It is clear that PFD_{avg} results can change an entire SIL level or more when all critical variables are not used.